1 Mbps coherent one-way QKD with dense wavelength division multiplexing and hardware key distillation

Nino Walenta,[1] Andreas Burg,[2] Jeremy Constantin,[2] Nicolas Gisin,[1] Olivier Guinnard,[1] Raphael Houlmann,[1] Charles Ci Wen Lim,[1] Tommaso Lunghi,[1] and Hugo Zbinden[1]

[1] *Group of Applied Physics-Optique, University of Geneva, Chemin de Pinchat 22, 1211 Geneva, Switzerland*

[2] *Telecommunications Circuits Laboratory, École Polytechnique Fédérale de Lausanne, 1015 Lausanne, Switzerland*

We present the latest results obtained with a quantum cryptography prototype based on a coherent-one way quantum key distribution (QKD) scheme. To support its continuous high rate secret key generation we developed different low-noise single photon detectors for telecom wavelength based on a sine gating and low-pass-filtering technique, as well as a negative feedback APD in an active hold-off circuit. A newly developed hardware distillation engine allows for continuous operation of secret key distribution up to 1 Mbps. We also present results of our system in a DWDM (dense wavelength-division multiplexing) configuration where only one single fiber is needed to interconnect Alice' and Bob's systems. The final prototype is fully compatible to serve a high-speed encryption device developed in parallel which provides encrypted communication of up to 100 Gbps.

I. INTRODUCTION

Quantum key distribution (QKD) [1] is the most complex and advanced application of quantum physics adopted commercially today. Improving the reliability, performance and transmission distances of direct point-to-point quantum communication systems in optical telecom networks is a challenge which requires not only optimized QKD protocols, robust optical setups and appropriate single photon detectors, but also fast post-processing engines to distill the secret key. In the scope of the NanoTera QCRYPT project [2] we are implementing an integrated QKD prototype based on the coherent-one-way QKD scheme [3, 4], fast low-noise single photon detectors [5, 6] and a hardware key distillation engine completely implemented in a FPGA (field-programmable gate array). Here, we present the latest results showing the performance of the system for high rate quantum key distribution to continuously distill secret keys with rates larger than 1 Mbps (megabit per second). We compare the results obtained with recently developed sine-gated single photon detectors and low-noise free-running detectors and implement the system in a standard 2-fiber configuration as well as a 1-fiber-only DWDM configuration as shown in Fig. 1. We furthermore present the results and discuss the advantages and limits of hardware key distillation and apply recent results on key recycling in authentication [7] in a finite key scenario of our protocol.

II. THE 625 MBPS COHERENT-ONE-WAY QKD SYSTEM

A sketch of the implemented coherent-one way QKD [3] system is shown in Fig. 1. It belongs to the class of so called phase-distributed QKD protocols which promise high secret key rates with simple hardware. Alice encodes random bits based on the output of a quantum random number generator into weak coherent states arranged in pairs of time bins. A logical bit of information is encoded by sequences of an empty time bin and a time bin with a coherent state of amplitude α, namely $|\beta_0\rangle := |0\rangle|\alpha\rangle$ and $|\beta_1\rangle := |\alpha\rangle|0\rangle$. By the definition of coherent states, these states have a fidelity of $\langle\beta_0|\beta_1\rangle = e^{-|\alpha|^2}$ which implies that any attempt to distinguish between them is probabilistic. In addition, Alice can also randomly prepare a decoy sequence $|\alpha\rangle|\alpha\rangle$ which contains no bit value but assures security of the key transmission. With Bob's measurement device we unambiguously discriminate the bit states by measuring the time-of-arrival of the photons in the single photon detector D_{bit} to obtain the raw key bits, or measure the coherence between successive states using an imbalanced interferometer and detector D_{mon} to ensure the security. The presence of an eavesdropper thus is detected by a loss of coherence and the potential eavesdropping information measured by a reduction in the interference visibility.

III. FAST LOW NOISE NEAR-INFRARED SINGLE PHOTON DETECTORS

Fast, efficient and robust near-infrared single photon detectors with high detection rates, low timing jitter and low noise contributions due to dark count or afterpulsing play a crucial part in many quantum optical communication systems. Although in the past years alternative detection techniques, e.g. based on cryogenically cooled superconducting

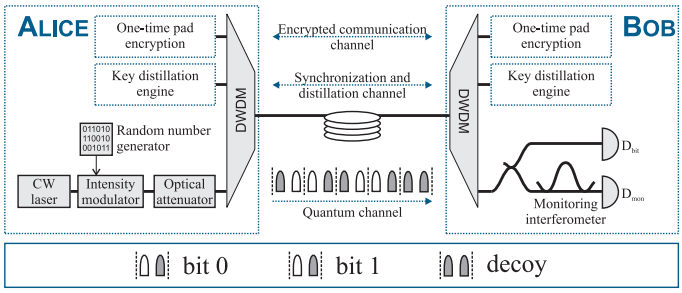

FIG. 1: Schematic of the implemented QKD system based on a coherent-one way protocol. The quantum states are prepared by Alice with a frequency of 625 Mbps and detected by Bob using fast SPADs (D_{bit} and D_{mon}) which are capable to discriminate between two time bins separated by only 800 ps. In the presented DWDM configuration all classical channels needed for synchronization, distillation and encrypted communication are wavelength multiplexed together with the quantum channel to require only one single fiber link between Alice and Bob.

nanowires or sum-frequency generation , have been successfully implemented, InGaAs/InP single photon avalanche diodes (SPADs) are today's preferred choice for detectors in integrated systems due to their compactness, robustness and reliability [8, 9]. Besides their advantages, one of the factors limiting the performance of InGaAs/InP SPADs is the afterpulsing effect and several approaches have been taken to mitigate the impairment in quantum communication setups [9, 10]. Recently, new gating schemes have been proposed and implemented which are based on very short gating periods during which the detector is sensitive for single photon detection. These short gates largely reduce the number of charge carriers generated during an avalanche and, hence, the afterpulse probability, while at the same time allowing for high gate frequencies and detection rates [11].

We present recent results characterizing a single photon avalanche detector using a sine gating scheme with a simple but effective low-pass filtering technique for fast low-noise single photon detection at telecom wavelength. The detector is characterized by 130 ps short gates applied with a frequency of 1.25 GHz, yields only 70 ps timing jitter and noise probabilities as low as $7 \cdot 10^{-7}$ per gate at 10 % detection efficiency (see Fig. 2). We show that the detector is suitable for high rate quantum key distribution and even at room temperature it could allow for QKD over distances larger than 25 km [5]. Another approach to counter afterpulsing has recently been commercialised [12] based on a diode integrating monolithically a feedback resistor. This solution effectively quenches the avalanche and drastically reduces afterpulsing. We implemented and characterized a detector module based on this diode in an active hold-off circuit which further reduces the afterpulsing and notably improves the detector performances. We demonstrate free-running operation with 600 Hz dark count rate at 10 % detection effciency [6] and compare its performance with the sine-gating technique in a 2-fiber and 1-fiber-only DWDM configuration as shown in Fig. 1.

IV. KEY DISTILLATION ENGINE

The quantum key distribution process is accompanied by classical communication between Alice and Bob over an authenticated public channel to distill secret keys from the raw detections. This classical communication comprises sifting, parameter estimation, error correction and verification, privacy amplification and authentication. To perform all classical post-processing with sufficiently high throughput such that the QKD process can run continuously, we have developed a hardware key distillation engine based on FPGAs (Xilinx Virtex 6).

This engine uses a forward error correction scheme using a quasi-cyclic LDPC code based on syndrome encoding [13]. It can efficiently correct errors over a wide range of error rates by adapting its code rates. Such, the effective throughput decreases only by 0.5 % if the QBER is increased to 6 %. For privacy amplification we use an implementation based on Toeplitz matrice multiplication [14] which allows for adjusting the compression ratio to the channel parameters by scaling the output block size. Prior to privacy amplification, an integrity check is required since the error detection capability of the forward error correcting scheme is insufficient to guarantee that all errors have been corrected. The chosen mechanism consists in applying a universal hash function [15, 16] on each key block. Thanks to the use of randomness, this construction ensures that the integrity check mechanism cannot be guessed in advance by Eve.

Recently, the impact of key recycling in authentication was analyzed where the same hash function is reused for multiple authentication rounds while information leakage about the particular hash function used is limited by one-time-pad encryption of the tags attached to the messages [7]. There, it was proven that this authentication scheme is ϵ-universal-composable secure if ϵ-almost strongly universal_2 hash functions are used and bound for its information leakage is derived. We use this result and implement it in a finite key analysis [17] of our system.

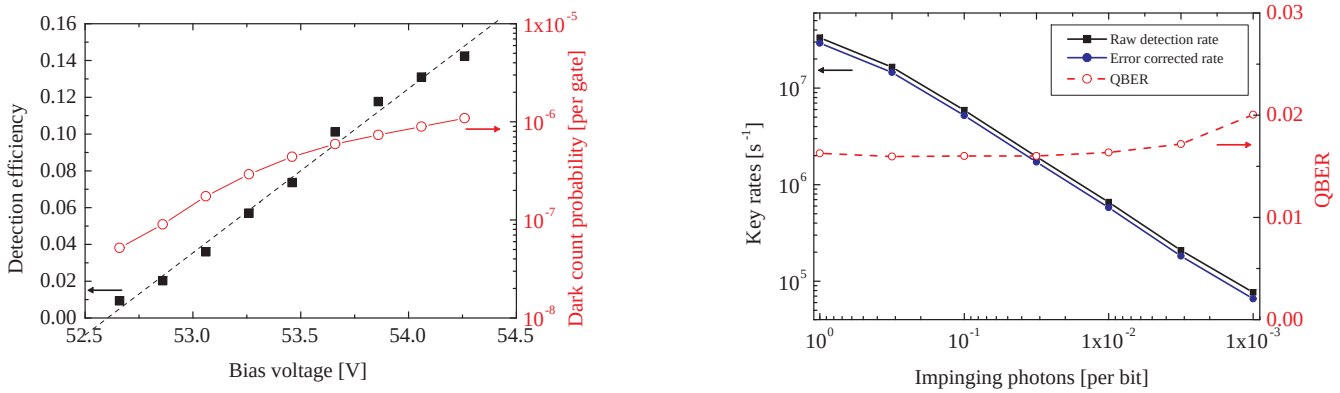

FIG. 2: Left: Detection efficiency (squares) and dark count probability per gate (circles) as the function of bias voltage. For a detection efficiency of 0.1 we measure a dark count probability as low as $6 \cdot 10^{-7}$ per gate of 130 ps (FWHM) width. Right: Detection rates and quantum bit error rates (QBER) for the 1.25 GHz sine gated APD in a QKD scenario. From the measured raw detection rates and QBER we estimate a COW secret key rate [4] larger 1 Mbps up to 4 dB fiber losses (corresponding to 20 km standard fiber length.)

V. CONCLUSION

We present recent results of a fully integrated QKD system based on the coherent one way protocol. The system employs low-noise single photon detectors which yield only 70 ps timing jitter and noise probabilities as low as $7 \cdot 10^{-7}$ per gate at 10 % detection efficiency. We present the implementation of our hardware key distillation engine and show that it can continously achieve 1 Mbps secret key rate over more than 10 km fiber distance.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics **74**, 145 (2002).
[2] `http://www.nano-tera.ch/projects/404.php`.
[3] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Applied Physics Letters **87**, 194108 (2005).
[4] C. Branciard, N. Gisin, and V. Scarani, New Journal of Physics **10**, 013031 (2008).
[5] N. Walenta, T. Lunghi, O. Guinnard, R. Houlmann, H. Zbinden, and N. Gisin, submitted (2012), arXiv:1205.3084v1 [quant-ph].
[6] T. Lunghi, C. Barreiro, O. Guinnard, R. Houlmann, X. Jiang, M. A. Itzler, and H. Zbinden, to appear in J. Mod. Opt. (2012), arXiv:1204.4594v1 [physics.ins-det].
[7] C. Portmann, arXiv:1202.1229v1 [cs.IT] (2012).
[8] R. T. Thew, N. Curtz, P. Eraerds, N. Walenta, J. D. Gautier, E. Koller, J. Zhang, N. Gisin, and H. Zbinden, Nuclear Instruments & Methods **610**, 16 (2009).
[9] M. A. Itzler, X. Jiang, M. Entwistle, K. Slomkowski, A. Tosi, F. Acerbi, F. Zappa, and S. Cova, Journal of Modern Optics **58**, 174 (2011).
[10] S. Cova, A. Lacaita, and G. Ripamonti, IEEE Electron Device Letters **12**, 685 (1991).
[11] J. Zhang, P. Eraerds, N. Walenta, C. Barreiro, R. Thew, and H. Zbinden, Proceedings of the SPIE - The International Society for Optical Engineering p. 76810Z (8 pp.) (2010).
[12] M. A. Itzler, X. Jiang, B. Nymann, and K. Slomkowski, Proc. SPIE 2009 (2009).
[13] C. Roth, P. Meinerzhagen, C. Studer, and A. Burg, in *Solid State Circuits Conference (A-SSCC), 2010 IEEE Asian* (2010), pp. 1–4.
[14] H. Krawczyk, in *Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology* (Springer-Verlag, 1994), CRYPTO '94, pp. 129–139, ISBN 3-540-58333-5.
[15] J. L. Carter and M. N. Wegman, Journal of Computer and System Sciences **18**, 143 (1979).
[16] M. N. Wegman and J. L. Carter, Journal of Computer and System Sciences **22**, 265 (1981), URL `http://www.sciencedirect.com/science/article/pii/0022000081900337`.
[17] C. C. W. Lim, *Finite key analysis of a simple and efficient one-way quantum cryptography system*, in preparation.